(19) JAPANESE PATENT OFFICE

JPA 08-221364

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08221364 A**

(43) Date of publication of application: **30.08.96**

(51) Int. Cl **G06F 15/00**
G06F 13/00

(21) Application number: **07026456**

(22) Date of filing: **15.02.95**

(71) Applicant: **HITACHI LTD**

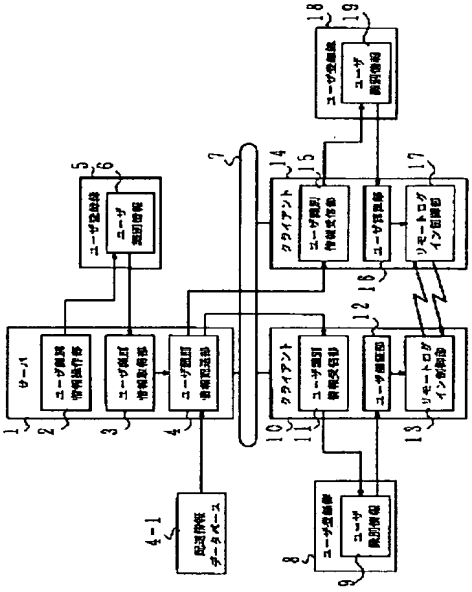
(72) Inventor: **KOBAYASHI SHIGEYUKI**
HAYASHI TOMONORI
MORI YASUKO

(54) DECENTRALIZED MANAGEMENT METHOD FOR USER REGISTRATION BOOK

(57) Abstract:

PURPOSE: To guarantee the consistency of user identification information among plural systems and to reduce the operation management work for a user registration book on a network system.

CONSTITUTION: A server 1 and clients 10 and 14 constituting a computer system connected through the network system 7 are provided and a means (user identification information operation part 2) for operating the user registration book 5 is present only in the server 1. A user identification information distribution part 4 for distributing the user identification information 6 operated in the server 1 through the network system 7 is present on the server 1, a user identification information reception part 11 is provided on the client 10 and the user identification information reception part 15 is provided on the client 14 for reflecting the distributed user identification information on respective user registration books 8 and 18.



JPA08-221364

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－221364

(43)公開日　平成８年(1996)８月30日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
G06F 15/00	330	9364-5L	G06F 15/00	330	B
13/00	357	7368-5E	13/00	357	Z

審査請求　未請求　請求項の数１　ＯＬ　（全７頁）

(21)出願番号　特願平7－26456

(22)出願日　平成７年(1995)２月15日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　小林　茂之
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　林　朋典
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　森　八寿子
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

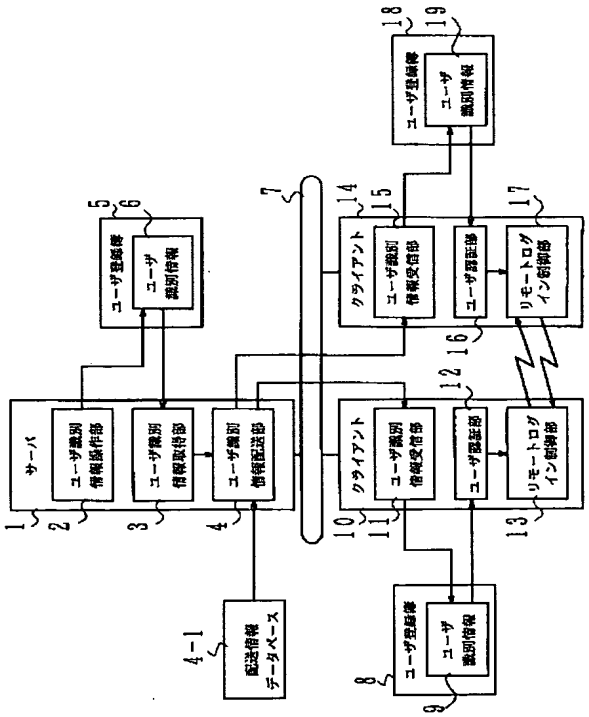
(74)代理人　弁理士　小川　勝男

(54)【発明の名称】ユーザ登録簿の分散管理方法

(57)【要約】

【目的】複数のシステム間でユーザ識別情報の一貫性を保証するとともに、ネットワークシステム上でのユーザ登録簿の運用管理作業を軽減する。

【構成】ネットワークシステム７を介して接続されたコンピュータシステムであるサーバ１とクライアント１０、１４があり、ユーザ登録簿５を操作する手段（ユーザ識別情報操作部２）がサーバ１のみに存在し、サーバ１で操作されたユーザ識別情報６をネットワークシステム７を介して配付するユーザ識別情報配送部４がサーバ１上に存在し、配付されたユーザ識別情報をユーザ登録簿８と１８にそれぞれ反映するために、クライアント１０上にユーザ識別情報受信部１１とクライント１４上にユーザ識別情報受信部１５を持つ。



1

【特許請求の範囲】

【請求項１】ネットワークシステムを介して複数のコンピュータシステムが接続されたユーザ登録簿の分散管理方法において、

ユーザのリモートログイン操作時に当該ユーザの認証に必要とされるユーザ識別情報を保持するユーザ登録簿を、登録サーバと呼ばれるコンピュータシステムで一元管理するため、

該登録サーバのみがユーザ識別情報を一括操作し、かつ該登録サーバで一括操作された更新ユーザ情報を上記ネットワークシステムを経由して各々のユーザ識別情報を保持するクライアントと呼ばれるコンピュータシステムに配送し、

該クライアントは上記更新ユーザ情報を受け取り、各自が保持するユーザ登録簿に該更新ユーザ情報を登録することを特徴とするユーザ登録簿の分散管理方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ネットワーク分散環境におけるユーザ登録簿の分散管理方法に関し、特に複数コンピュータ相互間でリモートログインを許可するか否かの手続きを簡単化し、かつユーザ認証情報の一貫性を保証することができるユーザ登録簿の分散管理方法に関する。

【０００２】

【従来の技術】近年、ネットワークシステムを介してワークステーションからパーソナルコンピュータ、メインフレーム等のコンピュータシステムを接続し、大規模なシステムを構築する場合が増加している。このような環境の中で、これらのシステム相互間でリモートログイン等のサービスを提供するためには、ユーザ登録簿によるユーザの認証が必要である。なお、リモートログインとは、複数のコンピュータが相互接続されている場合に、１つのコンピュータを介して他のコンピュータのプログラムやデータを使用することであり、その際の認証とは、あるユーザが常時使用しているコンピュータＡを経由して他のコンピュータＢを使用する際に、そのコンピュータＢの使用を要求することにより、そのコンピュータＢがそのユーザを使用させてよいか否かを許可する手続きを言う。この場合、一般に個々のコンピュータシステムでユーザ登録簿を管理することによる管理作業の増大が問題となっている。

【０００３】図２は、従来のネットワークシステム上で行われているユーザ登録簿の管理方法の例を示す図である。図２では、サーバ２０、クライアント２７、２８の３つのコンピュータシステムがネットワークシステム２６で接続されている。これらの３つのコンピュータシステムでは、共通なユーザ識別情報２５がユーザ登録簿２４に保持されており、サーバ２０のみがユーザ登録簿２４を操作することができる。サーバ２０はユーザ登録簿

2

２４中のユーザ識別情報の一部または全てに対して、追加、削除、更新などの操作を行うために必要なユーザ識別情報操作部２１を有する。いま、クライアント２７のリモートログイン制御部３１がユーザの指示によってクライアント２８にリモートログインしようとする場合、リモートログイン制御部３１はクライアント２８上のリモートログイン制御部３４とネットワークシステム２６を介して接続される。クライアント２８上のリモートログイン制御部３４は、クライアント２７上のリモートログイン制御部３１からログインを要求するユーザを認証するため、ユーザ認証部３３を呼び出す。ユーザを認証するためのユーザ識別情報２５はサーバ２０に接続されたユーザ登録簿２４上にのみ存在するため、クライアント２８のユーザ認証部３３はユーザ識別情報要求部３２を呼び出す。ユーザ識別情報要求部３２はネットワークシステム２６を介して、サーバ２０上のユーザ識別情報管理部２３と通信し、ユーザ識別情報管理部２３はユーザ識別情報取得部２２を呼び出し、ユーザ登録簿２４から当該ユーザのユーザ識別情報を得る。クライアント２８のユーザ認証部３３は、取得したユーザ識別情報を元にクライアント２７のユーザを認証し、リモートログインを許可するか否かを決定する。なお、クライアント２８上のユーザがクライアント２７にリモートログインする時も、全く同様の手続きを行うことにより、ユーザ登録簿２４の保持するユーザ識別情報２５をサーバ２０に問い合わせ、リモートログインを許可するか否かが決定される。この方法では、リモートログイン時のユーザ認証のために、サーバへの問い合わせが必須となる。

【０００４】図３は、他の従来例を示すもので、ユーザ登録簿を個々のホストで別々に管理する場合を示している。図３では、ホスト３５、４４、４８の３つがネットワークシステム４１を介して接続されており、それぞれのホストにユーザ登録簿３９、４２、５２が接続されている。これらの３つのユーザ登録簿３９，４２，５２には、ユーザ識別情報４０、４３、５３がそれぞれ保持されており、また各ホストは、各々のユーザ識別情報の一部または全てに対して、追加、削除、更新などの操作を行うために必要なユーザ識別情報操作部３６、４７、５１の３つを備えている。ホスト３５のリモートログイン制御部３８が、ユーザの指示によってホスト４４にリモートログインしようとする場合、リモートログイン制御部３８はホスト４４上のリモートログイン制御部４５とネットワークシステム４１を介して接続される。ホスト４４上のリモートログイン制御部４５は、リモートログイン制御部３８からログインを要求するユーザを認証するため、ユーザ認証部４６を呼び出す。ユーザ認証部４６ではユーザ登録簿４２に保持されたユーザ識別情報４３から当該ユーザのユーザ識別情報を取得し、ホスト３５上のユーザを認証し、リモートログインを許可するか否かを決定する。この方法では、ホスト毎にユーザ登録

簿が保持され、リモートログインが要求されたホスト上で、リモートログインを要求するユーザの認証が行われる。なお、この種のネットワーク上でのユーザ登録簿の管理方法については、例えば「ＳＵＮシステム管理」（株式会社アスキー　平成３年３月２０日発行）のＰ．２０３からＰ．２０７までに記載されている。

【０００５】

【発明が解決しようとする課題】図２で例示される従来の方法では、クライアントシステム２７や２８がリモートログインを要求するユーザを認証するためには、サーバ２０にネットワークシステム２６を介して問い合わせる必要があった。このため、サーバ２０が故障などの原因で使用不可能になると、ネットワークシステム２６に接続されたクライアント２７、２８、サーバ２０の相互のコンピュータシステム間で、リモートログイン機能が全く使えなくなるという弱点があった。また、この従来方法では、管理されるコンピュータシステムの数が増加すると、サーバ２０への問い合わせ数が増大し、ネットワークシステム２６上のネットワーク性能に悪影響を与えるとともに、システムの可用性を低下させる場合があるという問題点があった。図３で例示される従来の方法では、ユーザ識別情報が個々のホストで別々に管理されているため、ネットワーク上でのユーザ認証情報の一貫性を保つためには、同じユーザの認証情報をそれぞれのユーザ登録簿に別々に登録する必要があるという無駄があった。つまり、ユーザ識別情報の操作が必要な場合には、ホスト３５、４４、４８のそれぞれでユーザ識別情報操作部３６、４７、５１を使用して、ユーザ識別情報４０、４３、５３を更新する必要があった。従って、ネットワークシステム４１に接続されるホスト数が増加するに伴って、ユーザ識別情報の更新に必要な管理作業も増加するという問題があった。本発明の目的は、このような従来の課題を解決し、複数ホストに対するユーザ認証情報の一貫性を保証することができるとともに、複数ホストのユーザ登録簿を更新するための作業を軽減することができるユーザ登録簿の分散管理方法を提供することにある。

【０００６】

【課題を解決するための手段】上記の目的を達成するため、本発明によるユーザ登録簿の分散管理方法では、ユーザ識別情報を操作するための唯一の手段であるユーザ識別情報操作部をネットワークシステム上の一つのサーバのみに置き、ユーザ識別情報操作部からの指示により、更新されたユーザ識別情報をユーザ識別情報配送部から配送し、ユーザ識別情報受信部がユーザ識別情報配送部からユーザ識別情報を受け取り、ユーザ登録簿に登録することによって、ユーザ識別情報を一括管理する。また、それぞれのホストに接続されたユーザ登録簿の情報でユーザを認証することによって、サーバへの問い合わせのためのトラヒック量を削減することができる。

【０００７】

【作用】本発明においては、ユーザ識別情報を操作するユーザ識別情報操作部をネットワークシステム上の一つのサーバのみに配置することにより、ネットワークで接続された複数のコンピュータでユーザの認証のために使われるユーザ識別情報をサーバで一括して操作することを可能としている。また、サーバで操作されたユーザ識別情報をネットワークで接続されたコンピュータシステムに配布する手段をサーバに持たせることによって、各コンピュータのユーザ登録簿にユーザ識別情報を配布することを可能にしている。この結果、ユーザ登録簿をそれぞれのコンピュータシステムで別々に管理する場合に比べて、ユーザ登録簿の運用管理にかかる作業を軽減することができる。また、リモートログイン時のユーザの認証において、それぞれのコンピュータに独立して配置されたユーザ登録簿中のユーザ識別情報を元に当該ユーザを認証することによって、ネットワークシステムのサーバなどに依存すること無く、ネットワーク上の個々のコンピュータシステムで、独立してユーザの認証を可能としている。この結果、本発明では、リモートログインを要求するユーザを認証する時に、サーバにのみユーザ登録簿を配置する方法に比べて、クライアントコンピュータからサーバへのネットワーク経由で通信する処理を無くすることができ、サーバの障害発生によりリモートログインサービスが使用出来なくなるような不都合を無くすることができる。

【０００８】

【実施例】以下、本発明の実施例を、図面により詳細に説明する。図１は、本発明の一実施例を示すユーザ登録簿の分散管理システムの構成図である。図１では、サーバ１、クライアント１０、クライアント１４の３つのコンピュータシステムが、ネットワークシステム７で接続されている。ユーザ登録簿５、８、１８は、サーバ１、クライアント１０、クライアント１４でそれぞれ別々に保持されている。図３に示す従来方法との違いは、図３ではユーザ登録簿中のユーザ識別情報を操作するための手段であるホスト３５、ホスト４４、ホスト４８がユーザ識別情報操作部３６、４７、５１をそれぞれ別々に保持していたのに対し、図１では、ユーザ識別情報操作部３６がホスト３５にのみ保持されている点である。これを、図３に適用すると、ユーザ登録簿３９、４２、５２中のユーザ識別情報４０、４３、５３の管理をすべてホスト３５のユーザ識別情報操作部３６により実施することを意味する。但し、図１では、ユーザ登録簿５、８、１８中のユーザ識別情報６、９、１９の一貫性を保つため、サーバ１のユーザ識別情報操作部２で操作されたユーザ識別情報６を配布するための手段として、サーバ１はユーザ識別情報取得部３とユーザ識別情報配送部４を持っている。また、サーバ１から配送されるユーザ識別情報を受け取り、ユーザ登録簿８と１８に反映するため

に、クライアント１０と１４はそれぞれユーザ識別情報受信部１１と１５を持っている。

【０００９】まず、ユーザ識別情報の操作は、サーバ１上のユーザ識別情報操作部２の指示によって、ユーザ登録簿５中にユーザ識別情報６として反映される。次に、サーバ１のユーザ識別情報取得部３は前記操作で更新されたユーザ識別情報６をユーザ識別情報配送部４に渡す。ユーザ識別情報配送部４は、配送情報データベース４－１の情報を参照し、ユーザ識別情報を配送すべきホストとしてクライアント１０と１４を探しだし、ネットワークシステム７を介してユーザ識別情報６を、クライアント１０のユーザ識別情報受信部１１と、クライアント１４のユーザ識別情報受信部１５にそれぞれ渡す。ユーザ識別情報を受け取ったクライアント１０とクライアント１４のユーザ識別情報受信部１１と１５は、それぞれユーザ登録簿８とユーザ登録簿１８にその情報を反映する。このようにして、サーバ１上だけでユーザ識別情報の操作を可能にするので、サーバ１、クライアント１０、クライアント１４のユーザ識別情報６、９、１９の一貫性を保つことが可能となる。

【００１０】４図は、ユーザ識別情報の配送を制御するための配送情報データベースの一例を示すフォーマット図である。４図で示されるように、配送情報データベース４－１には、ユーザ毎にビット０からビットｎまでのビットマップをテーブルとして持っている。各ビットは、本発明でユーザ登録簿を管理するホストに対応している。つまり、ビット０はホストＡ、ビット１はホストＢ、ビット２はホストＣ、ビット３はホストＤ、ビットｎはホストｎのように対応する。ビット０～ｎの位置に‘１’が立っているときユーザが使用できるコンピュータを持つホストであり、‘０’が立っているときユーザが使用できないコンピュータを持つホストであることを意味している。例えば、ユーザＡ（５４）は、ホストＢ、ホストＥを使用できること、ユーザＢ（５５）はホストＡ、ホストＥを使用できること、ユーザＣ（５６）は、ホストＣ、ホストＤ、ホストＥを使用できること、ユーザＤ（５７）は、ホストＡ～ホストｎまでの全ホストを使用できることをそれぞれ表わしている。

【００１１】従って、システム側から見た場合におけるそれぞれのビットの意味は、当該ユーザ名のユーザ識別情報に変更がなされた場合に、当該ユーザのユーザ識別情報を配送すべきホストかどうかを示している。例えば、ビット０が１であるならば、ホストＡにユーザ識別情報を配送する必要があることを示し、ビット０が０であるならば、ホストＡにユーザ識別情報を配送する必要がないことを示す。本実施例では、ユーザＡ５４、ユーザＢ５５、ユーザＣ５６、ユーザＤ５７が図４に明示されている。そして、ユーザＡはビット０が０、ビット１が１、ビット２が０、ビット３が０、ビット４が１であり、ビットｎが０であることが図４に示されている。このことは、ユーザＡ５４のユーザ識別情報がサーバ１で変更された場合、ビット１が１であるホストＡとビット４が１であるホストＤにユーザＡ５４のユーザ識別情報を配送するということを示す。

【００１２】次に、本実施例におけるリモートログイン時のユーザの認証については、図３で示された従来方法と同等の方法で実現する。図１では、クライアント１０上のユーザがクライアント１４にリモートログインしようとする場合には、クライアント１０のリモートログイン制御部１３がユーザの指示によって、クライアント１４にリモートログインしようとする場合、リモートログイン制御部１３はクライアント１４上のログイン制御部１７とネットワークシステム７を介して接続される。クライアント１４上のリモートログイン制御部１７は、リモートログイン制御部１３からログインを要求するユーザを認証するために、ユーザ認証部１６を呼び出す。ユーザ認証部１６ではユーザ登録簿１８に保持されたユーザ識別情報１９から当該ユーザのユーザ識別情報を取得し、クライアント１０上のユーザを認証し、リモートログインを許可するか否かを決定する。この方法では、ホスト毎にユーザ登録簿が保持され、リモートログインが要求されたホスト上でユーザの認証が行われるため、図２で示された方法のようなサーバへの問い合わせによるネットワークトラヒック量の増加や、リモートログインができなくなるといった問題を解消することができる。

【００１３】

【発明の効果】以上説明したように、本発明によれば、ネットワークシステム上で複数のホストに接続されたユーザ登録簿の更新情報を各ホストに配布する唯一の手段を設けたため、複数ホストに対するユーザ認証情報の一貫性を保証することができ、かつサーバへの問い合わせ数も増大することなく、複数ホストのユーザ登録簿を更新するための作業を軽減するという効果を有する。

【図面の簡単な説明】

【図１】本発明の一実施例を示すユーザ登録簿分散管理システムの構成図である。

【図２】従来例を示すものであって、サーバでユーザ登録簿を管理し、クライアントとサーバの協調によりユーザを認証するシステムの構成例図である。

【図３】従来例を示すものであって、各ホストで別々にユーザ登録簿を管理し、各ホストでユーザを認証するシステムの構成例図である。

【図４】図１におけるユーザ識別情報の配送に使用される配送情報データベースの内容の一例を示す図である。

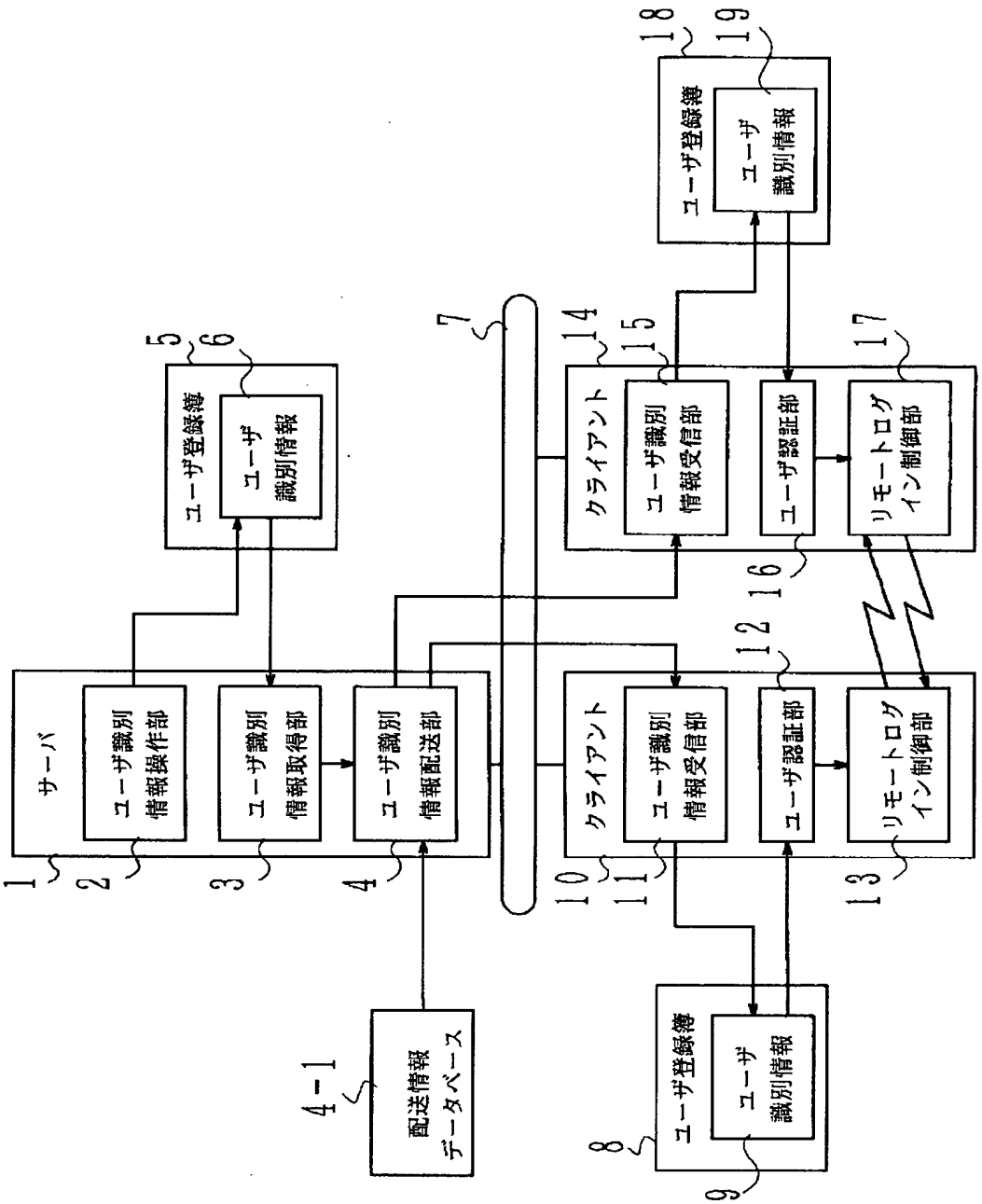
【符号の説明】

１…サーバ、２…ユーザ識別情報操作部、３…ユーザ識別情報取得部、４…ユーザ識別情報配送部、５，８，１８…ユーザ登録簿、６，９，１９…ユーザ識別情報、７…ネットワークシステム、８…ユーザ登録簿、１０，１４…クライアント、１１，１５…ユーザ識別情報受信

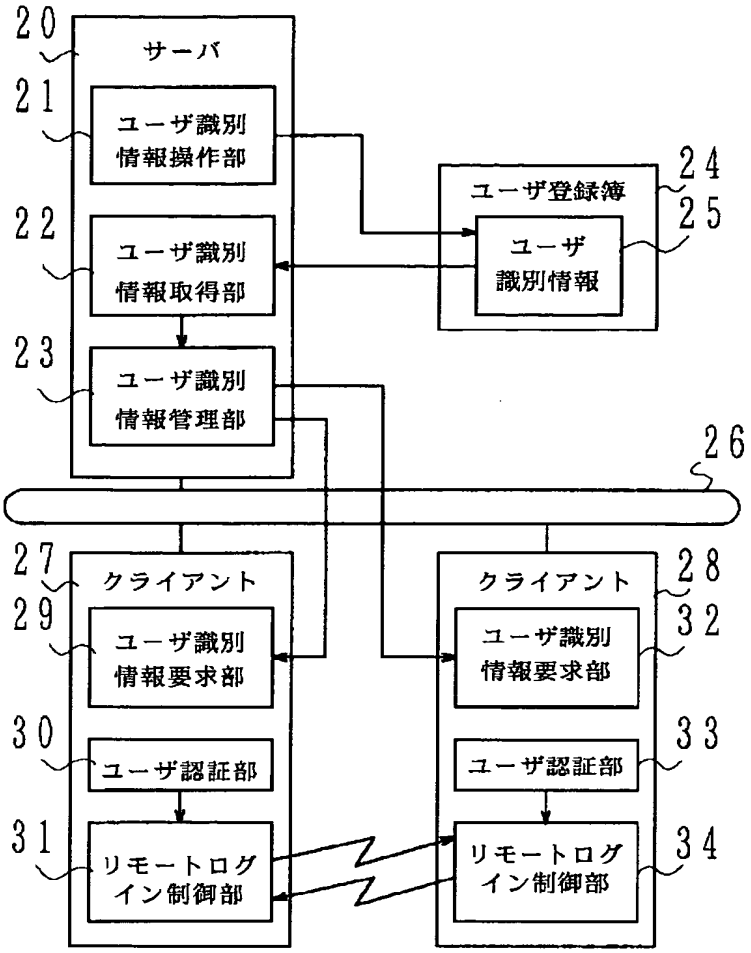
7　　8

部、１２，１６…ユーザ認証部、１３，１７…リモートログイン制御部、４－１…配送情報データベース、２０…サーバ、２７，２８…クライアント、３５，４４，４８…ホスト。

【図１】



【図２】

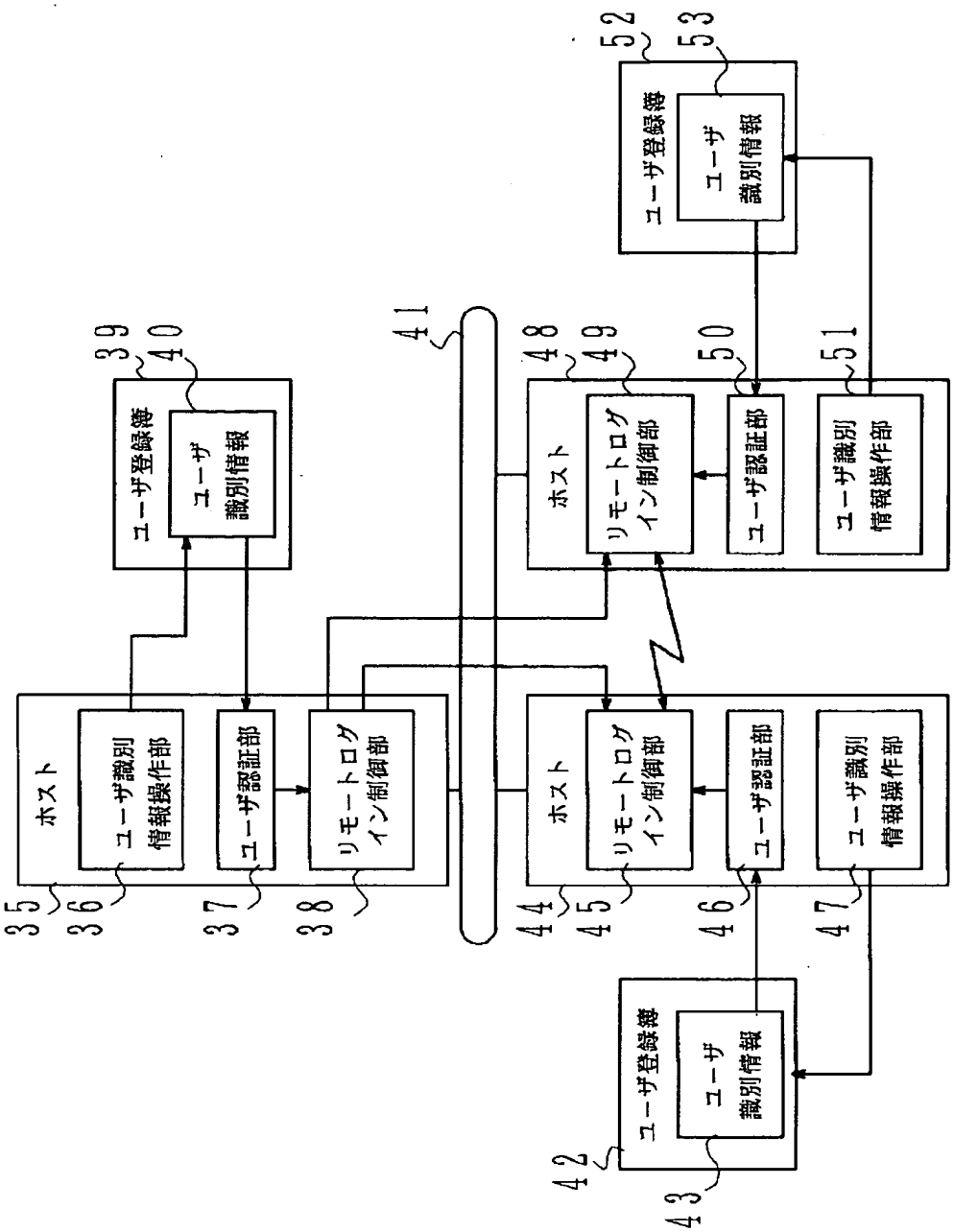


【図４】

58 配送情報データベース

	ホストA	ホストB	ホストC	ホストD	ホストE	・・・	ホストn
ビット	0	1	2	3	4		n
54 ユーザA	0	1	0	0	1		0
55 ユーザB	1	0	0	0	1		0
56 ユーザC	0	0	1	1	1		0
57 ユーザD	1	1	1	1	1		1
⋮							

【図３】


ホスト
ユーザ識別情報操作部
ユーザ認証部
リモートログイン制御部
ユーザ登録簿
ユーザ識別情報
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53